REMARKS/ARGUMENTS

The Examiner rejects claims 13-14, 23, 26-32, 34-41, and 44-45 under 35 U.S.C.§102(e) as being anticipated by U.S. Patent 6,772,333 to Brendel; claims 2-7, 11, 16-20, 24, 37, and 42 under 35 U.S.C.§103(a) as being anticipated by Brendel in view of U.S. Patent 6,516,416 to Gregg et al.; claims 8-9 and 21-22 under 35 U.S.C.§103(a) as being unpatentable over Brendel in view of Schneier; and claims 10, 33, 38, and 43 under 35 U.S.C.§103(a) as being unpatentable over Brendel in view of U.S. Patent 5,923,885 to Johnson et al.

Applicant respectfully traverses the Examiner's rejections. Brendel, Gregg et al., Schneier, and Johnson et al. fail to teach or suggest, individually and collectively, at least the following italicized features of the pending independent claims:

> 36. A method of communication data between a first computing device and a second computing device, the method comprising:
>
> (a) a browser on the first computing device providing a Web page to a user, the Web page comprising at least first and second input fields for input from the user and at least a first presentation field associated with the at least first and second input fields and wherein the Web page displays simultaneously to the user the first and second input fields;
>
> (b) a program on the first computing device receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the Web page, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, and wherein the first datum comprises at least one of a credit card number and a social security number;
>
> (c) *the program identifying that the first datum is confidential and the second datum is non-confidential*;
>
> (d) *the first computing device communicating, to the second computing device over an untrusted network, the first datum with encryption*; and

(e) *the first computing device communicating, to the second computing device over the untrusted network, the second datum without encryption, wherein steps (d) and (e) occur at least substantially simultaneously.*

40. A system for communicating data between first and second computing devices, comprising:

(a) a first computer device operable to communicate data over an untrusted network, the first computer device comprising:

a user display, the display comprising, at one time, at least first and second input fields of a Web page for input from the user and at least a first presentation field associated with the at least first and second input fields;

means for receiving a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user, wherein the first datum comprises at least one of a credit card number and a social security number; and

means for identifying that the first datum is confidential and the second datum is non-confidential; and

(b) a second communication device in communication with the first communication device, wherein the first computing device communicates, to the second computing device over the untrusted network, *the first datum with encryption and the second datum without encryption.*

44. A method of communicating data between a first computing device and a second computing device, the method comprising the steps of:

at a first computing device, receiving input information from one Web page displayed to a user, the input information comprising at least first and second datum corresponding respectively to at least first and second user input fields, wherein the first datum comprises at least one of a credit card number and a social security number;

at the first computing device, *a program determining which of the at least first and second user input fields contains confidential information, wherein the first datum is confidential to the user and the second datum is not confidential to the user*;

the first computing device communicating the first datum of the message to a second computing device with encryption of the first datum; and

the first computing device communicating the second datum of the message over an untrusted network to the second computing device without encryption of the second datum.

45. A data communication system comprising:

(a) a first computer device operable to communicate data over an untrusted network, the first computer device comprising:

a user display, the display comprising at least first and second input fields of a single, displayed Web page for input from the user and at least a first presentation field associated with the at least first and second input fields;

an input operable to receive a message from the user, wherein the message comprises at least a first and second datum input by the user into the at least first and second input fields, respectively, of the display, wherein the first datum is confidential to the user and the second datum is non-confidential to the user and wherein the first datum comprises at least one of a credit card number and a social security number; and

a procedure operable to identify that the first datum is confidential and the second datum is non-confidential; and

(b) a second communication device in communication with the first communication device, wherein the first computing device communicates, to the second computing device over the untrusted network, *the first datum with encryption and the second datum without encryption.*

The present invention is directed to an encryption module that encrypts only part of a transmission sent by one node to another node. Specifically, a graphical display is presented to a user requesting the user to input information into a number of fields. Some of the fields are confidential while others are not. The fields are identified accordingly. When the user requests transmission of the displayed information to another node, the module encrypts only the confidential fields and not the non-confidential fields. The use of encryption on only part of the transmission can represent substantial savings in computational resources both at the transmitting and receiving nodes.

Brendel

Brendel is directed to a load balancer that assigns incoming requests to servers at a server farm. An atomic operation assigns both un-encrypted and clear-text requests and encrypted

requests from a client to the same server at the server farm. An encrypted session is started early by the atomic operation, before encryption is required. The atomic operation is initiated by a special, automatically loaded component on a web page. This component is referenced by code requiring that an encrypted session be used to retrieve the component. Keys and certificates are exchanged between a server and the client to establish the encrypted session. The server generates an SSL session ID for the encrypted session. The server also generates a server-assignment cookie that identifies the server at the server farm. The cookie is encrypted and sent to the client along with the SSL session ID. The client decrypts the cookie and stores it along with the SSL session ID. The load balancer stores the SSL session ID along with the server assignment that identifies the server that generated the SSL ID. When the other encrypted requests are generated by the client to the server farm, they include the SSL ID. The load balancer uses the SSL session ID to send the requests to the assigned server. When the client sends a non-encrypted clear-text request to the server farm, it includes the decrypted server-assignment cookie. The load balancer parses the clear-text request to find the server-assignment cookie. The load balancer then sends the request to the assigned server.

Brendel does not disclose sending different information from different fields of a common Web page in two different forms, namely encrypted (for confidential information) and unencrypted (for nonconfidential information). The Examiner relies the following passages for this teaching:

. . .

> Less critical data such as product descriptions and advertisements can be sent as non-encrypted data, while only the more critical data such as credit-card numbers are encrypted. The non-encrypted or clear-text data can be sent using standard or clear-text TCP/IP connections while the encrypted data is sent using an encrypted session. [col. 1, lines 37-42]
>
> . . .
>
> Once the user decides to buy a product, types in his credit card information, and presses a 'submit' button, an encrypted session (session 3) begins with encrypted connection 1. Other clear-text connections (clear text connection 3) for non-critical information may be started or in progress. [col. 1, lines 53-58]
>
> . . .
>
> A typical e-commerce web site provides clear-text web pages to users that show and describe products (catalog pages). The user can select a product for purchase by checking a check box or button on the product description page or a page with a list of products. Often the user continues to browse other products after a product has been selected for purchase. The selected product is put into a database maintained on the server, while the user continues to browse, perhaps adding other items to his "shopping cart".
>
> Eventually the user is ready for check-out, and clicks a "buy now" or other button to finish the purchase. The user then begins an encrypted session and is asked to enter the credit card or other payment and shipping instructions. [col. 10, lines 21-34]
>
> . . .
>
> When the user is ready to check out, encrypted request 64 is sent by the client to the server farm. [col. 11, lines 46-47]
>
> . . .

Contrary to the Examiner's conclusions, the above language does not mean that confidential and nonconfidential information in the *same* Web page are sent encrypted and unencrypted, respectively. Rather, the language simply means that Web pages containing

confidential information (alone or in addition to nonconfidential information) are encrypted in their entireties while Web pages containing nonconfidential information only are sent unencrypted in their entireties.

A number of passages of Brendel support this conclusion.

By way of example, Brendel states:

> Eventually the user is ready for check-out, and clicks a "buy now" or other button to finish the purchase. The user then begins an encrypted session and is asked to enter the credit card or other payment and shipping instructions.

(Col. 10, lines 31-36.)

> One server keeps a list of all items added to the shopping cart by clear-text connections, and also processes the encrypted connections at checkout. Thus servers do not have to pass the shopping cart list to other servers at the server farm.

(Col. 10, lines 52-55.)

This passage states that, prior to establishing the encrypted session, the Web pages and information contained therein are sent in clear text. After the encrypted session is established, the Web pages are sent encrypted.

Moreover, Brendel states, at col. 13, lines 33-40, that:

> Current load balancers can only persist encrypted sessions. By enabling persistent user sessions consisting of clear-text and encrypted connections, encryption is not necessarily used for product-information pages or other noncritical information. Only financial or personal information such as credit card numbers may be encrypted. This reduces the computational effort required by the servers since fewer encrypted *pages* are served.

(Emphasis supplied.) This passage makes clear that entire Web pages, and not subsets of information on the Web pages, are sent either unencrypted or encrypted.

These passage describe a common e-commerce configuration in which Web pages containing one or more confidential fields are encrypted in their entireties while Web pages not containing one or more confidential fields are not encrypted at all. They do not say that only flagged portions of Web pages are encrypted while unflagged portions are not encrypted or vice versa.

The remaining references fail to overcome the deficiencies of Brendel.

Gregg et al.

Gregg et al., the other primary reference, is directed to a system for controlling the access to computer resources using an untrusted network. The system uses a hardware key connected to each subscriber client computer and adds software to the client computer and to the existing server computer. A clearinghouse is provided to store client and server identification data, including demographic data, URL data, usage data, and billing information. The clearinghouse authenticates the subscriber and server computers before an operating session occurs. For every new client session, a login mechanism requires the client computer to supply appropriate authentication data, including a digital identification generated by the hardware key. The login parameters are verified by the clearinghouse and a session is then started. The system is adapted to protect a preselected content from being printed or copied by a client using a web browser. The system architecture permits a geographical distributed system of multiple subscriber client

computers, multiple server computers and multiple clearinghouses which can interact with one another.

Gregg et al. uses login parameters, namely user name, password, and digital ID, to perform two-factor authentication. (Col. 7, lines 59-65; col. 14, lines 48-58; col. 17, lines 30-37.) Gregg et al. states:

> The subscriber software 36 accepts messages from the web server 69 and takes actions as commanded by the server such as making the subscriber login, polling for the optional access key, *encrypting the login parameters* and sending it to the server, performing URL tracking, and enforcing copyright protection.

(Col. 9, lines 6-12 (emphasis supplied).)

Gregg et al. further states, at col. 13, lines 44-46:

> The login parameters obtained from the user and the access key 54 are encrypted using the challenge sent by the login CGI 68, and sent back to the login CGI 68.

Gregg et al. further states at col. 17, lines 30-37:

> The login interface then sends the login parameters, *including the user name, password, and digital ID* to the client cryptographer (block 148). The client cryptographer encrypts the password and the digital ID using the challenge sent by the login enforcer and sends them to the login enforcer (block 150). The login enforcer then sends an initiate session message to the session initiator with the encrypted login parameters (block 152).

(Emphasis supplied.) Although the Examiner relies on this passage and element 3 of Fig. 2 for the teaching that the architecture of Gregg et al. encrypts only the password and digital ID and not the user name, this passage and Figure, taken in the context of the other passages, does not teach this. Rather Gregg et al. teach that all of the login parameters are encrypted and sent over

the untrusted network. In the above passage and in box 148 of Fig. 18, if the user name is not to be encrypted why is it sent to the client cryptographer? The Examiner has failed to answer this question because it is inconsistent with his position. Box 152 of Fig. 18, in fact, states that "Log-In Enforcer Sends Initiate Session (IS) Message to Session Initiator with the *Encrypted Log-In Parameters*." (Emphasis supplied.)

Finally, Gregg et al. states at col. 25, lines 50-58:

> In order to perform subscriber authentication, the subscription access server will need to interact with the system clearinghouse 30, which it does by establishing and maintaining a communication line between itself and the clearinghouse. The information transmitted on this communication line [which includes the log-in parameters] is encrypted using a public/private key mechanism so that only authentic servers and an to [sic] authentic subscription access clearinghouse can communicate with each other.

Based on the foregoing, it is clear that all of the login parameters sent to the client cryptographer are encrypted. Nowhere does Gregg et al. say that the user name is *not* encrypted as one of the log-in parameters.

Johnson et al.

Johnson et al. is directed to a method for dynamically modifying a browser interface to provide software functionalities that are distributed from a server across a network to a user working on a client computer which is coupled to the server through the computer network. Applets are downloaded onto a browser client. The applets are software code that is executed by the browser already running on the client. In this manner, software is distributed in a platform

independent manner that allows users to execute software without having that software installed on their local machines.

Accordingly, the pending claims are allowable.

The dependent claims provide further reasons for allowance.

By way of example, dependent claim 2 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the step of communicating the first datum with encryption and the second datum without encryption in a same packet that comprises the message. *See also* dependent Claims 16, 37, and 42. Contrary to the Examiner's statements, this feature is neither suggested nor disclosed by the cited references as noted above.

Dependent claim 3 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the message without encryption of the second datum to include the steps of communicating the first datum with encryption in a first packet of the message and communicating the second datum without encryption in a second packet of the message different from the first packet of the message. *See also* dependent Claim 17. Contrary to the Examiner's statements, this feature is neither suggested nor disclosed by the cited references as noted above.

Dependent claim 4 requires the step of communicating the first datum of the message with encryption of the first datum and the step of communicating the second datum of the

message without encryption of the second datum comprise the step of employing a same path between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claims 18, 38 and 43. Contrary to the Examiner's statements, this feature is neither suggested nor disclosed by the cited references as noted above.

Dependent claim 5 requires the step of employing the same path to communicate the first datum with encryption and the second datum without encryption to include the step of employing a TCP/IP passage between the first computing device and the second computing device to communicate the first datum with encryption and the second datum without encryption. *See also* dependent Claim 19. Contrary to the Examiner's statements, this feature is neither suggested nor disclosed by the cited references as noted above.

Dependent claim 6 requires the step of communicating the first datum of the message with encryption of the first datum to include the step of employing a key to encrypt the first datum of the message for communication of the first datum from the first computing device to the second computing device with encryption of the first datum. *See also* dependent Claims 7-9 and 20-22. Contrary to the Examiner's statements, this feature is neither suggested nor disclosed by the cited references as noted above.

Dependent claim 10 requires the Web page to include hypertext markup language, the first datum to include the credit card number, the second datum to include information related to a purchase by the user and the program to be embedded in the Web page. The program is loaded

on the first computing device after the Web page is received by the first computing device. *See also* claims 33, 38, and 43. Because the cited references fail to teach or suggest the need to distinguish between confidential and nonconfidential information in the same Web page, there is no incentive or motivation to use the applet distribution mechanism of Johnson et al. in the architecture of Brendel to realize the claimed invention.

Dependent claim 41 requires the first and second datum to be communicated at least substantially simultaneously. Contrary to the Examiner's statements, this feature is neither suggested nor disclosed by the cited references as noted above.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: Nov. 21, 2005